

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims

1. (Currently Amended) A method for accessing data in a read/write storage medium within one of a plurality of storage cartridges mounted into a plurality of interface devices, comprising:

providing an association of at least one coding key to the plurality of storage cartridges, wherein the coding key associated with the storage cartridge is used to decode and code data in the storage cartridge;

encrypting the coding [[key]] keys and storing the encrypted coding keys in the storage cartridges;

receiving, by a receiving interface device comprising one of the interface devices, an Input/Output (I/O) request to a target storage cartridge comprising one of the storage cartridges; mounting, by the receiving interface device, the target storage cartridge in response to the I/O request;

reading, by the receiving interface device, the encrypted coding key from the mounted target storage cartridge;

transmitting, by the receiving interface device, the read encrypted coding key to a host device;

receiving, by the receiving interface device, the coding key encrypted by the host;

decrypting, by the receiving interface device devices, the encrypted coding key encrypted by the host to use for in response to the I/O request;

using, by the receiving interface device devices, the decrypted coding key to decode data to read in the target storage cartridge associated with the decrypted including the encrypted coding key in response to the I/O request comprising a read request; and

using, by the receiving interface device devices, the decrypted coding key to code data to write to the target storage cartridge including the encrypted associated with the decrypted coding key in response to the I/O request comprising a write request.

2. (Canceled)

3. (Previously Presented) The method of claim 1, wherein the association of the at least one coding key to the plurality of storage cartridges associates one key with the plurality of storage cartridges, wherein the one key encodes data written to the storage mediums and decode data read from the storage mediums of the plurality of storage cartridges.

4. (Original) The method of claim 1, wherein the association of the at least one coding key to the plurality of storage cartridges associates a different key with each storage cartridge, wherein the key associated with one storage cartridge is used to encode data written to the storage medium and decode data read from the storage medium of the storage cartridge.

5. (Original) The method of claim 1, wherein the coding key comprises a seed value that is used to generate an additional key that is used to directly decode and encode the data in the storage medium in the storage cartridge.

6. (Canceled)

7. (Currently Amended) The method of claim [[6]] 1, wherein encrypting the coding key further comprises:

encrypting, by the host, the coding key with a first key, wherein the interface devices use a second key to decrypt the coding key encrypted with the first key.

8. (Currently Amended) The method of claim [[6]] 1, wherein encrypting the coding key further comprises:

encrypting the coding key with a first key, wherein the host uses a second key ~~is used~~ to decrypt the coding key encrypted with the first key, wherein the host encrypts the coding key by encrypting the ~~second coding~~ key with a third key, wherein the interface devices uses a fourth key to decrypt the coding key data encrypted by the host with the third key; ~~and transmitting the coding key encrypted with the first key and the second key encrypted with the third key to the interface device.~~

9. (Canceled)

10. (Currently Amended) A method performed by an interface device for accessing data in a removable storage cartridge including a read/write storage medium coupled to the interface device, comprising:

receiving an encrypted coding key from a host system with an Input/Output (I/O) request directed to the storage cartridge;

mounting the storage cartridge in response to the I/O request;

decrypting the encrypted coding key;

using the decrypted coding key to encode data to write to the storage medium in response to the I/O request comprising a write request;

using the decrypted coding key to decode data written to the storage medium in response to the I/O request comprising a read request; and

storing the received encrypted coding key in the storage medium to use for subsequent I/O requests.

11. (Previously Presented) The method of claim 10, wherein encoding the data with the coding key compresses the data and wherein decoding the data written to the storage medium decompresses the data, and wherein the data is only encoded or decoded using the coding key.

12. (Currently Amended) The method of claim 10, wherein the coding key is encrypted by a first key maintained at the host system, further comprising:

maintaining, by the interface device, a second key to decrypt data encrypted using the first key, wherein the interface device uses the second key ~~is used~~ to decrypt the coding key encrypted with the first key.

13. (Original) The method of claim 12, wherein the second key is stored in an integrated circuit non-volatile memory that is only accessible to decrypting logic that uses the second key to decrypt data encrypted using the first key.

14. (Original) The method of claim 13, further comprising:

transmitting the coding key decrypted using the decrypting logic to encoder/decoder logic, wherein the encoder/decoder logic uses the coding key to encode and decode data to the storage medium.

15. (Original) The method of claim 12, further comprising:
storing the coding key encrypted with the first key within the storage cartridge;
receiving an input/output (I/O) request directed to the storage cartridge; and
accessing the encrypted coding key from the storage cartridge, wherein the accessed coding key is decrypted using the second key, and wherein the decrypted coding key is used to encode and decode data to execute the I/O request to the storage cartridge.

16. (Currently Amended) The method of claim 10, wherein the received encrypted coding key is encrypted by a first key maintained at the host system, wherein the host system maintains a second key to decrypt data encrypted using the first key, wherein the interface device decrypts the encrypted coding key by further comprising:

receiving, with the I/O request, from the host system, the second key encrypted by the host system using a third key, wherein data encrypted using the third key is decrypted using a fourth key;

accessing the fourth key;

using the fourth key to decrypt the encrypted second key received from the host system;
and

using the decrypted second key to decrypt the received coding key encrypted using the first key.

17-43. (Canceled)

44. (Previously Presented) The method of claim 1, wherein the storage cartridges comprise tape media and the data on the storage cartridges coded and decoded using the at least one coding key comprises archival data.

45. (New) The method of claim 8, wherein the first key comprises a host public key, wherein the second key comprises a host private key, wherein the third key comprises an interface device public key and wherein the fourth key comprises an interface device private key.

46. (New) The method of claim 16, wherein the first key comprises a host public key, wherein the second key comprises a host private key, wherein the third key comprises an interface device public key and wherein the fourth key comprises an interface device private key.

47. (New) A system for accessing data in a read/write storage medium within one of a plurality of storage cartridges and to communicate with a host, comprising:

an interface device having a controller for performing operations, the operations comprising:

receiving an Input/Output (I/O) request to a target storage cartridge comprising one of the storage cartridges, wherein at least one coding key is associated with the plurality of storage cartridges, wherein the coding key associated with the storage cartridge is used to decode and code data in the storage cartridge, and wherein encrypted coding keys are stored in the storage cartridges;

mounting the target storage cartridge in response to the I/O request;

reading the encrypted coding key from the mounted target storage cartridge;

transmitting the read encrypted coding key to a host device;

receiving the coding key encrypted by the host;

decrypting the coding key encrypted by the host to use for the I/O request;

using the decrypted coding key to decode data to read in the target storage cartridge including the encrypted coding key in response to the I/O request comprising a read request; and

using the decrypted coding key to code data to write to the target storage cartridge including the encrypted coding key in response to the I/O request comprising a write request.

48. (New) The system of claim 47, wherein the association of the at least one coding key to the plurality of storage cartridges associates one key with the plurality of storage cartridges, wherein the one key encodes data written to the storage mediums and decode data read from the storage mediums of the plurality of storage cartridges.

49. (New) The system of claim 47, wherein the association of the at least one coding key to the plurality of storage cartridges associates a different key with each storage cartridge,

wherein the key associated with one storage cartridge is used to encode data written to the storage medium and decode data read from the storage medium of the storage cartridge.

50. (New) The system of claim 47, wherein encrypting the coding key further comprises:

encrypting, by the host, the coding key with a first key, wherein the interface devices use a second key to decrypt the coding key encrypted with the first key.

51. (New) The system of claim 47, wherein encrypting the coding key further comprises:

encrypting the coding key with a first key, wherein the host uses a second key to decrypt the coding key encrypted with the first key, wherein the host encrypts the coding key by encrypting the coding key with a third key, wherein the interface devices uses a fourth key to decrypt the coding key encrypted by the host with the third key.

52. (New) The system of claim 47, wherein the storage cartridges comprise tape media and the data on the storage cartridges coded and decoded using the at least one coding key comprises archival data.

53. (New) The system of claim 51, wherein the first key comprises a host public key, wherein the second key comprises a host private key, wherein the third key comprises an interface device public key and wherein the fourth key comprises an interface device private key.

54. (New) A system for accessing data in a removable storage cartridge including a read/write storage medium and in communication with a host system, comprising:

an interface device having a controller for performing operations, the operations comprising:

- receiving an encrypted coding key from the host system with an Input/Output (I/O) request directed to the storage cartridge;
- mounting the storage cartridge in response to the I/O request;
- decrypting the encrypted coding key;

using the decrypted coding key to encode data to write to the storage medium in response to the I/O request comprising a write request;
using the decrypted coding key to decode data written to the storage medium in response to the I/O request comprising a read request; and
storing the received encrypted coding key in the storage medium to use for subsequent I/O requests.

55. (New) The system of claim 54, wherein the coding key is encrypted by a first key maintained at the host system, wherein the operations further comprise:

maintaining a second key to decrypt data encrypted using the first key, wherein the interface device uses the second key to decrypt the coding key encrypted with the first key.

56. (New) The system of claim 55, wherein the second key is stored in an integrated circuit non-volatile memory that is only accessible to decrypting logic that uses the second key to decrypt data encrypted using the first key.

57. (New) The system of claim 56, wherein the operations further comprise:
transmitting the coding key decrypted using the decrypting logic to encoder/decoder logic, wherein the encoder/decoder logic uses the coding key to encode and decode data to the storage medium.

58. (New) The system of claim 55, wherein the operations further comprise:
storing the coding key encrypted with the first key within the storage cartridge;
receiving an input/output (I/O) request directed to the storage cartridge; and
accessing the encrypted coding key from the storage cartridge, wherein the accessed coding key is decrypted using the second key, and wherein the decrypted coding key is used to encode and decode data to execute the I/O request to the storage cartridge.

59. (New) The system of claim 54, wherein the received encrypted coding key is encrypted by a first key maintained at the host system, wherein the host system maintains a second key to decrypt data encrypted using the first key, wherein the interface device decrypts the encrypted coding key by:

receiving, with the I/O request, from the host system, the second key encrypted by the host system using a third key, wherein data encrypted using the third key is decrypted using a fourth key;

accessing the fourth key;

using the fourth key to decrypt the encrypted second key received from the host system;

and

using the decrypted second key to decrypt the received coding key encrypted using the first key.

60. (New) The system of claim 59, wherein the first key comprises a host public key, wherein the second key comprises a host private key, wherein the third key comprises an interface device public key and wherein the fourth key comprises an interface device private key.

61. (New) An article of manufacture comprising at least one of a computer readable storage media and hardware including an Input/Output (I/O Manager) and controller for accessing data in a read/write storage medium within one of a plurality of storage cartridges mounted into a plurality of interface devices, wherein the controller and I/O manager are executed to perform:

providing, by the I/O manager, an association of at least one coding key to the plurality of storage cartridges, wherein the coding key associated with the storage cartridge is used to decode and code data in the storage cartridge;

encrypting, by the I/O manager, the coding keys and storing the encrypted coding keys in the storage cartridges;

receiving, by the controller, an Input/Output (I/O) request to a target storage cartridge comprising one of the storage cartridges;

mounting, by the controller, the target storage cartridge in response to the I/O request;

reading, by the controller, the encrypted coding key from the mounted target storage cartridge;

transmitting, by the controller, the read encrypted coding key to a host device;

receiving, by the controller, the coding key encrypted by the host;

decrypting, by the controller, the coding key encrypted by the host to use for the I/O request;

using, by the controller, the decrypted coding key to decode data to read in the target storage cartridge including the encrypted coding key in response to the I/O request comprising a read request; and

using, by the controller, the decrypted coding key to code data to write to the target storage cartridge including the encrypted coding key in response to the I/O request comprising a write request.

62. (New) The article of manufacture of claim 61, wherein the association of the at least one coding key to the plurality of storage cartridges associates one key with the plurality of storage cartridges, wherein the one key encodes data written to the storage mediums and decode data read from the storage mediums of the plurality of storage cartridges.

63. (New) The article of manufacture of claim 61, wherein the association of the at least one coding key to the plurality of storage cartridges associates a different key with each storage cartridge, wherein the key associated with one storage cartridge is used to encode data written to the storage medium and decode data read from the storage medium of the storage cartridge.

64. (New) The article of manufacture of claim 61, wherein the coding key comprises a seed value that is used to generate an additional key that is used to directly decode and encode the data in the storage medium in the storage cartridge.

65. (New) The article of manufacture of claim 61, wherein encrypting the coding key further comprises:

encrypting, by the I/O manager, the coding key with a first key, wherein the controller uses a second key to decrypt the coding key encrypted with the first key.

66. (New) The article of manufacture of claim 61, wherein encrypting the coding key further comprises:

encrypting the coding key with a first key, wherein the host uses a second key to decrypt the coding key encrypted with the first key, wherein the host encrypts the coding key by

encrypting the coding key with a third key, wherein the controller uses a fourth key to decrypt the coding key encrypted by the host with the third key.

67. (New) The article of manufacture of claim 61, wherein the storage cartridges comprise tape media and the data on the storage cartridges coded and decoded using the at least one coding key comprises archival data.

68. (New) An article of manufacture comprising at least one of a computer readable storage media and hardware including an Input/Output (I/O Manager) and controller for accessing data in a read/write storage medium within one of a plurality of storage cartridges mounted into a plurality of interface devices, wherein the controller and I/O manager are executed to perform:

- receiving, by the controller, an encrypted coding key from the I/O manager with an Input/Output (I/O) request directed to the storage cartridge;
- mounting, by the controller, the storage cartridge in response to the I/O request;
- decrypting, by the controller, the encrypted coding key;
- using, by the controller, the decrypted coding key to encode data to write to the storage medium in response to the I/O request comprising a write request;
- using, by the controller, the decrypted coding key to decode data written to the storage medium in response to the I/O request comprising a read request; and
- storing, by the controller, the received encrypted coding key in the storage medium to use for subsequent I/O requests.

69. (New) The article of manufacture of claim 68, wherein encoding the data with the coding key compresses the data and wherein decoding the data written to the storage medium decompresses the data, and wherein the data is only encoded or decoded using the coding key.

70. (New) The article of manufacture of claim 68, wherein the coding key is encrypted by a first key maintained by the I/O manager, wherein the operations further comprise:

- maintaining, by the controller, a second key to decrypt data encrypted using the first key, wherein the interface device uses the second key to decrypt the coding key encrypted with the first key.

71. (New) The article of manufacture of claim 70, wherein the second key is stored in an integrated circuit non-volatile memory that is only accessible to decrypting logic that uses the second key to decrypt data encrypted using the first key.

72. (New) The article of manufacture of claim 71, wherein the operations further comprise:

transmitting, by the controller, the coding key decrypted using the decrypting logic to encoder/decoder logic, wherein the encoder/decoder logic uses the coding key to encode and decode data to the storage medium.

73. (New) The article of manufacture of claim 70, wherein the operations further comprise:

storing, by the controller, the coding key encrypted with the first key within the storage cartridge;

receiving, by the controller, an input/output (I/O) request directed to the storage cartridge;
and

accessing, by the controller, the encrypted coding key from the storage cartridge, wherein the accessed coding key is decrypted using the second key, and wherein the decrypted coding key is used to encode and decode data to execute the I/O request to the storage cartridge.

74. (New) The article of manufacture of claim 68, wherein the received encrypted coding key is encrypted by a first key maintained by the I/O manager, wherein the I/O manager maintains a second key to decrypt data encrypted using the first key, wherein the controller decrypts the encrypted coding key by:

receiving, with the I/O request, from the I/O manager the second key encrypted by the I/O manager using a third key, wherein data encrypted using the third key is decrypted using a fourth key;

accessing the fourth key;

using the fourth key to decrypt the encrypted second key received from the I/O manager
and

using the decrypted second key to decrypt the received coding key encrypted using the first key.

75. (New) The article of manufacture of claim 74, wherein the first key comprises a host public key, wherein the second key comprises a host private key, wherein the third key comprises an interface device public key and wherein the fourth key comprises an interface device private key.